Department of Budget and Management
Office of Information Technology

Information Technology
Security Policy and Standards
Version 1.3

December 2005

Table of Contents

Introduction

This document provides policy and supporting standards for information technology (IT) security. The policy applies to Executive agencies of the State of Maryland, and establishes general requirements and responsibilities for protecting technology systems, including the responsibility for each agency to have its own technology security plan. The standards establish minimum levels of compliance.

The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, and many other more specialized resources. The policy is necessitated by the State's use of IT to help carry out nearly all of its public services and internal operations. The State's delivery of critical public services depends on the availability, reliability and integrity of its IT systems. Therefore each agency must adopt appropriate methods to protect its technology systems. While some agencies will need to adopt stronger standards and methods, the statewide program based on this policy provides the minimum requirements and a consistent approach for security.

The common security approach also supports compatible security solutions shared among agencies, yielding a better return on technology investment. The security policy and standards will evolve and will require regular updates to remain current.

The Secretary of the Department of Budget and Management issues the policy and standards under authority granted by the Annotated Code of Maryland, Finance and Procurement Article § 3-401 through 3-413 and § 3-701 through 3-705. The Office of Information Technology within the Department of Budget and Management administers the policy.

Persons with questions or needing further information are encouraged to contact the Information Technology Security Officer in the Office of Information Technology (410-260-7778).

Section: 1	Revision: 2
Date Adopted: June 2003	Date Revised: December 2005

1 Information Technology Security Policy

Information and information technology systems are essential assets of the State of Maryland. They are vital to the citizens of the State. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as to local and federal government entities and to other State agencies. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Each agency of the Executive Branch of the State is responsible for compliance with this policy and these standards. The Office of Information Technology (OIT) of the Department of Budget and Management and agency IT components are to use this policy and these standards as a guide when procuring IT services, service providers, contractors, software, hardware and network components.

1.1 Scope

This policy covers all information that is electronically generated, received, stored, printed, filmed, and typed. In accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, the provisions of this policy apply to:

- All units of the Executive Branch of the State of Maryland for all of their IT systems regardless of who is operating them;
- All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights.

1.2 Objectives

This policy and these standards define the minimum requirements to which each State agency, including employees and contractors, must adhere. The primary objectives of the IT Security Policy are:

- To establish a secure environment for the processing of data;
- To reduce information security risk;
- To communicate the responsibilities for the protection of information.

1.3 Previous Policy Superseded

This policy and these standards supersede the policies and standards as previously stated in the “State Agency Data Systems Security Practices” as revised (1999).

1.4 Authority

The Office of Information Technology of the Department of Budget and Management has authority to set policy and provide guidance and oversight for security for all IT systems in accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705.

1.5 Compliance

The head of each agency is responsible for compliance with and enforcement of this policy. Agency Chief Information Officers (CIOs) shall develop and implement an Agency IT Security Program to implement this policy and these standards. Where the agency's IT Security Program is unable to comply with this policy, a timetable to resolve the discrepancies and controls for compliance shall be included. The controls shall include but are not limited to:

- Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services;
- Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed;
- Ensuring that risks to information security are identified and controls implemented to mitigate these risks;
- Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards;
- Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations;
- Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's IT assets.

1.6 Security Program Maintenance and Review

Each State agency will review and update its IT Security Program as needed to conform to changes within the agency or in the State IT Security Program. Refer to NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems for additional guidance: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc. The status of agency IT Security Programs Systems shall be reported according to Section 4.9.

1.7 Information Technology Security Deviation and Risk Acceptance

Compliance with this policy shall be planned and achieved as promptly as possible. When an agency determines, in the course of planning or carrying out its IT Security Program, that it is not feasible or practical to comply with a provision or provisions of this policy and attendant standards, or to do so promptly, it shall document the deviation from policy or standards. The documentation, with a timetable for compliance when practicable, shall be prepared as an IT Security Deviation Request.

IT Security Deviation Requests must be filed in accordance with the specifications detailed in the State IT Security Deviation/Risk Acceptance Standard (see Section 11, IT Security Deviation/Risk Acceptance Standard). Such deviations require the approval of the agency CIO, the agency head and the State CIO.

Section: 2	Revision: 2
Date Adopted: June 2003	Date Revised: December 2005

2 Key Definitions

Term / Acronym	Definition
Acceptable Risk	A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accountability	A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.
Accreditation	The authorization and approval granted to operate a system or network in order to process sensitive data in an operational environment.
Agency	All units of the Executive branch excluding the University System of Maryland.
Authentication	The testing or reconciliation of evidence of a user's identity.
Authorization	The rights and permissions granted to an individual (or process), which enables access to a computer resource.
Authorized Software	Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.
Availability	Ensures the reliable and timely access to data or computing resources by the appropriate personnel.
Certification	A technical review made as part of and in support of the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. A judgment and statement of opinion that the accrediting official can use to officially accredit the system is produced.
CIO	Chief Information Officer.
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical systems.
Computer	An electronic, magnetic, optical, or other data processing device or system that performs logical, arithmetic, memory, or storage functions. It includes any data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.
Confidentiality	Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.
Data Remanence	Residual information left behind once media has been in some way erased.
Incident	Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.
Identification	Data uniquely labeling a user to a system.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

Term / Acronym	Definition
Information Custodian	The business function owner responsible for the information assets for a particular IT System.
Integrity	Freedom from corruption or unauthorized modification; internal and external consistency.
IT Systems	Automated systems: communications systems including wireless systems, computer systems, hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.
ITEPP	Information Technology Emergency Preparedness Plan, including the business continuity plan, the recovery plan and the business resumption plan.
MCERT	Maryland's Computer Emergency Response Team. Team to be activated in the event of a major IT related disaster.
Mobile Code	Code that can be transmitted across the network and executed by a recipient.
Network	A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.
Untrusted Network	Any network not controlled by the State agency.
NIST	National Institute of Standards and Technology.
Nonpublic	Nonpublic is information that is not subject to inspection and copying under the Maryland Public Information Act or federal law.
Non-repudiation	Authentication with a high assurance to be genuine and that can not subsequently be refuted.
OIT	Office of Information Technology within the Department of Budget and Management.
Perimeter Access	Access to all entry and exit points of the network, controlled by firewalls and other filtering mechanisms.
Policy	For purposes of this document means both Policy and Standards
Privacy	Information that is free from unauthorized intrusion.
Public	Information that may be inspected and copied under the Maryland Public Information Act.
Residual Risk	The portion of risk that remains after security measures have been applied.
Risk	The probability that a particular threat will exploit a particular vulnerability of an IT System.
SDLC	Systems Development Life Cycle as defined in the State of Maryland SDLC Methodology (http://www.dbm.maryland.gov/ Keyword: SDLC).
SIA	Service Interface Agreement
Software	Computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.
VoIP	Voice over Internet Protocol, providing telephony services over IP networks.

Section: 3	Revision: 1
Date Adopted: June 2003	Date Revised: December 2005

3 Responsibility Standard

The following standard sets the minimum level of responsibility for the following individuals and/or groups:

- State CIO;
- Divisions of Security and Enterprise Architecture for OIT;
- Agency;
- Employees and Contractors.

3.1 State Chief Information Officer

The duties of the State CIO are:

- Providing Statewide IT security policy, standards, guidelines, and procedures;
- Ensuring the State's IT Security Program is established and implemented in compliance with State laws and regulations and federal laws where applicable;
- Approving deviations to IT security requirements;
- Reporting to the Governor and the Legislature on the status of the State's IT Security Program;
- Enforcing State security policy, including establishing the appropriate measures and remedial actions for agencies for non-compliance.

3.2 Divisions of Security and Enterprise Architecture, DBM OIT

These divisions are responsible for**:**

- Developing and maintaining a Statewide Security Program that includes policy, standards, guidelines, procedures, best security practices, IT disaster recovery planning guidelines, IT Security Certification and Accreditation guidelines, security awareness training, and an incident response reporting capability;
- Identifying security vulnerabilities in State systems and recommending corrective action;
- Ensuring IT Disaster Recovery plans for critical IT Systems are maintained and that plans are exercised at least annually;
- Developing and maintaining a Statewide security architecture;
- Coordinating with State agency CIO's, federal and local government, and private industry to resolve security issues and improve security for State systems;
- Provide the appropriate guidance to assist agencies in establishing IT Security Programs and compliance with IT Security Policy;
- Working with other State agencies to establish a coordinated computer incident response effort.

3.3 Agency Responsibilities

Each agency is responsible for:
Ensuring the agency's IT Security Program is established and implemented in compliance with State security policies and standards, State and federal laws and regulations as applicable;

- Implementing an IT Security Certification and Accreditation process for the life cycle of each

agency critical IT System;

- Reporting to the OIT on the status of the agency's IT Security Program
- Enforcing the State IT Security Policy;
- Managing the program and initiating measures to assure and demonstrate compliance with security requirements;
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions;
- Assuming the lead role in resolving security and privacy incidents;
- Documenting and ensuring that a process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard;
- Specifying the level of security required to protect all information assets under their control to comply with this Policy;
- Generating any IT Information Security Deviation/Risk Acceptance request in accordance with Section 11;
- Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
- Ensuring a configuration/change management process is used to maintain the security of the IT system;
- Administering a virus prevention and incident reporting program that coordinates with Maryland's Computer Incident Response Team;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users.

3.4 Employees and Contractors

All employees and contract personnel are responsible for:

- Being aware of their responsibilities for protecting IT assets of their agency and the State;
- Exercising due diligence in carrying out the IT Security Policy;
- Being accountable for their actions relating to their use of all IT Systems;
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State.

Section: 4	Revision: 2
Date Adopted: June 2003	Date Revised: December 2005

4 Information Technology Security Program Standard

Each agency is responsible for developing an IT Security Program for securing the agency's communications systems, computer systems, networks, and data in accordance with the State IT Security Policy. The status of an agency IT Security Program will be reported to the State CIO on an annual basis. This standard specifies the major components that must be included in every IT Security Program. The following list is not exhaustive; it functions as the minimum set of requirements. At a minimum each program must contain the following elements:

- IT Security Policy;
- Risk Management;
- Systems Development Life Cycle Methodology;
- IT Security Certification and Accreditation;
- IT Disaster Recovery Planning;
- IT Security Awareness Training;
- IT Incident Response Process;
- External Connections Review;
- IT Security Program Reporting.

4.1 IT Security Policy

Each agency must have a written IT security policy, with standards, and procedures. The agency policy must meet the minimum requirements as set forth in this policy.

4.2 Risk Management

A risk management process must be implemented to assess the acceptable risk to agency IT systems as part of a risk-based approach used to determine adequate security for the system. Agencies shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Agencies will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system (see Section 5, Nonpublic Information Standard). Refer to NIST Special Publication 800-30, Risk Management Guide for Information Technology for guidance: http://csrc.nist.gov/publications/nistpubs/.

4.3 Systems Development Life Cycle Methodology

All State systems must include IT security as part of the system development life cycle management process. Refer to the requirements in the State of Maryland SDLC Methodology: http://www.dbm.maryland.gov/: Keyword: SDLC.

4.4 IT Security Certification & Accreditation

Agencies shall develop and implement an IT security certification and accreditation program as part of an overall IT risk management strategy. The program will maintain a catalog of all IT systems and sites (to include existing), ranked by sensitivity and criticality. The cataloged items should be certified and accredited, in order, according to State IT Security Certification and Accreditation (C&A) Guidelines.

All new development shall be conducted using the IT Security C&A process integrated into the development process.

4.5 IT Disaster Recovery Planning

Agencies shall develop, implement, and test an IT Disaster Recovery plan for each critical IT system to ensure that a contingency system will be available in the event of a disaster to the primary production system. Reference State IT Disaster Recovery Guidelines.

4.6 IT Security Awareness, Training, and Education

Agencies shall develop and implement a security awareness, training, and education program for all agency employees and contractors to ensure that all employees and contractors adhere to the State IT Security Policy. Reference State IT Security Awareness Training and Education Training Guidelines.

4.7 IT Incident Response Process

Agencies shall be required to participate in the State Incident Response Process by detecting, tracking, logging, and reporting security incidents. Reference Maryland Computer Incident Response Capability Procedures and Standard Operation Procedures for Electronic Evidence Handling.

4.8 External Connections Review

External network connections, non-networked computers and dial-in connections shall be managed, reviewed annually, and documented as prescribed by the Agency IT Security Program. Results will be reported annually.

4.9 IT Security Program Reporting

Each agency is responsible for reporting on the status of the agency IT Security Program the DBM/OIT Security Division on an annual basis. A project plan detailing the projects, estimated costs, and estimated completion time required to bring the agency into compliance with the IT Security Policy must be included in the annual report.

Section: 5	Revision: 0
Date Adopted: June 2003	Date Revised:

5 Nonpublic Information Standard

Agencies shall establish and document a process that protects nonpublic information from disclosure to unauthorized individuals or entities, including other State or federal agencies. The process shall be compliant with the Maryland Public Information Act and any applicable federal laws.

5.1 System Sensitivity Designation

Each agency must specify corresponding classification and controls that must be in place for the data within that agency. When the IT System is shared between State units and/or between State, Federal, or local units the highest level of classification will determine the classification of the data or IT System. For example, one agency may categorize the data at a medium level while the second agency may classify the data at a basic level, therefore, the data at both agencies will be at a medium level. All parties sharing the IT System or data must agree to the initial classification and any change in the classification. An IT System shall clearly identify data that is considered non-public or public and any electronic exchange of data will clearly state that the information is non-public or public.

Section: 6	Revision: 1
Date Adopted: June 2003	Date Revised: December 2005

6 Access Control Standard

All Agencies must ensure that information is accessed by the appropriate persons for authorized use only. To help accomplish this each agency must establish at a minimum the following:

- An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system;
- An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and "need-to-know";
- An audit trail process to ensure accountability of system and security-related events;
- A process for ensuring that all systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, this capability must be enabled at all times;
- A review process of security audit logs, incident reports and on-line reports at least one (1) time per business day using automated tools to facilitate the review where possible;
- An investigation process for any unusual or suspicious items, which will incorporate reporting the results as specified in the State IT Incident Response Guideline;
- An internal assessment process for verifying their compliance to the State IT Security Policy;
- The processes to establish, manage, and document user id and password administration;
- A review of access privileges on an annual basis;
- A process for protecting nonpublic information;
- A process for explicitly authorizing access to nonpublic information;
- A process for documenting and escalating all instances of non-compliance with the State IT Security Policy;
- A segregation of the functions of system administration and security administration to provide separation of duties;
- Procedures prohibiting security personnel from initiating, programming, processing or authorizing business transactions;
- Independent audits of agency security administrators' security transactions.

6.1 Authentication

All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as "Functional ids". Functional ids are user accounts associated with a group or role that may be used by multiple individuals (e.g.. Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., RACF id used to run production jobs). Passwords associated with functional ids are exempt from the password restriction on sharing and change requirements specified below.

6.2 Password Construction Rules and Change Requirements

Passwords must meet the following usage, construction and change requirements:

- The password must not be the same as the user id;
- Passwords must never be displayed on the screen;
- The user must select passwords unless randomly generated. Initial passwords and password sets distributed to the user must be issued "pre-expired" forcing the user to change them upon

logon;

- Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters;
- Passwords must not contain leading or trailing blanks;
- Passwords must not contain more than two (2) consecutive identical characters;
- Password reuse must be prohibited by not allowing the last 10 passwords to be reused with a minimum password age of at least 2 days;
- Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
- Automated controls must ensure that passwords are changed at least as frequently as every ninety (90) days for regular users, forty-five (45) days for power users, such as network and database administrators;
- Passwords older than its expiration date must be changed before any other system activity is performed;
- User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts while allowing a minimum of a ten (10) minute automatic reset of the account;
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

6.3 Authorization

All Agencies must have the following authorization controls implemented:

- A documented process to ensure that access privileges are verified at least annually;
- An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity;
- A documented process to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hours of the change;
- A documented process to ensure that physical and logical access is immediately disabled upon a change in employment status where appropriate;
- An automated process to ensure that user ids are disabled after sixty (60) days of inactivity unless they are extended through the explicit approval of the Information Custodian (Note: Functional ids may be exempted from this requirement);
- A documented process to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use;
- A process/system to ensure that access privileges are traceable to a unique user id;
- An automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon.

6.4 Audit Trail

The following minimum set of events/actions must be logged and kept as required by State and Federal laws/regulations:

- Additions, changes or deletions to data produced by IT systems;
- Identification and authentication processes;
- Actions performed by system operators, system managers, system engineers, technical support, data security officers, and system administrators;
- Emergency actions performed by support personnel and highly privileged system and security resources.

The audit trails must include at least the following information:

- Date and time of event;
- User id of person performing the action;
- Type of event;
- Asset or resource name and type of access;
- Success or failure of event;
- Source (terminal, port, location, and so forth) where technically feasible.

6.5 Violation Log Management and Review

The Information Custodian must review all violations within one business day of a discovered occurrence. Automated tools are recommended when performing these review whenever possible. At a minimum the following events should be reviewed:

- Two (2) or more failed attempts per system day to access or modify security files, password tables or security devices;
- Disabled logging or attempts to disable logging;
- Two (2) or more failed attempts to access or modify nonpublic information within a week;
- Any unauthorized attempts to modify software or to disable hardware configurations.

Section: 7	Revision: 3
Date Adopted: June 2003	Date Revised: December 2005

7 Network Security Standard

Agencies must ensure that all information networks are protected from unauthorized access at all entry points. To help accomplish this, each agency must, at a minimum:

- Establish a process to protect from unauthorized dial-in access;
- Utilize the State approved banner text (See 7.2);
- Establish a process to ensure that all external IP connections are made through a firewall;
- Implement and monitor an Intrusion Detection Systems (IDS) or Intrusion Prevention System (IPS). Automated logging and reporting of this information should be 24x7x365;
- Establish a process to ensure that all Service Interface Agreements (SIAs) are managed in accordance with their IT Security Program and the State Policy;
- Establish a process to ensure that the same level of controls that exist on-site exist for users working remotely;
- Establish a process to prevent unauthorized mobile code from being loaded onto State IT equipment;
- Establish a process for ensuring that wireless network connections do not compromise the Agency's network;
- Establish a process for securing all Private Branch Exchanges (PBXs);
- Establish a process to prevent unauthorized networks to access VoIP networks.

7.1 Dial-in Access

The following services are prohibited except where they are specifically approved by the Agency CIO:

- Dial-in desktop modems;
- Use of any type of "remote control" product (e.g., PCAnywhere,GoToMyPC);
- Use of any network-monitoring tool.

In addition, the following controls for dial-in users must be implemented:

- Unique network access user ids different from their application or network user id;
- A minimum prohibition of answer or pickup until after the sixth (6^{th}) ring;
- Access privileges must be prohibited to any applications except those expressly required (i.e. cannot grant access to entire network, must be application specific);
- Annual review of access requirements;
- Shall not store data unless the data can be protected from unauthorized access, modification, or destruction.

7.2 Banner Text

The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs:

> *"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil*

penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose."

An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read. The banner is:

- Required for all mainframe, midrange, workstation, personal computer, and network systems;
- Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices;
- The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen. In such cases, this negative impact must be documented in the Agency's IT Security Program.

7.3 Firewalls & Network Devices

State networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. State firewalls should be configured to block all services not required, disable unused ports, hide and prevent direct access to State trusted network addresses from untrusted networks, prevent access by unauthorized source IP addresses or subnets, maintain comprehensive audit trails, fail in a closed state and operate on a dedicated platform (device).

All publicly accessible servers will be placed on a firewall interface configured as a DMZ. This DMZ must be separated from any interfaces connected directly to the internal network interface.

All network devices (e.g. servers, routers) shall have all non-needed services disabled and the security for those devices hardened. Publicly managed email and chat services will be prohibited inside an Agency network unless approved by the Agency CIO. All devices shall have updates and patches installed on a timely basis to correct significant security flaws. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

7.4 Intrusion Detection Systems

State networks will be monitored by an IDS or IPS implemented at critical junctures. Host-based, network-based, or a combination of both (preferred) may be utilized. IDS/IPS must be monitored and/or information logged 24x7x365. Each agency must establish a severity and escalation list based upon anticipated events that include immediate response capability when appropriate. These plans should be incorporated in the Agency's IT Security Program.

7.5 Service Interface Agreement

External network connections shall be permitted only after all approvals are obtained consistent with this policy and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system IT Security Certification and Accreditation package and in the IT System security plan. An SIA shall include:

- Purpose and duration of the connection as stated in the agreement, lease, or contract;
- Points-of-contact and cognizant officials for both the State and non-State organizations;
- Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations;
- Security measures to be implemented by the non-State organization to protect the State's IT

assets against unauthorized use or exploitation of the external network connection;
- Requirements for notifying a specified State official within a specified period of time of a security incident on the network, with the recommended time within 4 hours of the incident;
- A provision allowing the State to periodically test the ability to penetrate the non-state network through the external network connection or system.

7.6 Teleworking

In a telecommuting environment, an agency must require the same level of security on the microcomputer used at home or offsite as the microcomputer used in the workplace.

7.7 Mobile Code

Until reliable executable content scanning technology is available to address security concerns with regard to mobile code or executables obtained via the Web, all mobile code or executable content employed within a agency intranet shall be documented in the IT System Security Plan and approved by the Agency CIO.

7.8 Wireless Networks

7.8.1 General Controls

Each agency must:

- Complete a Certification and Accreditation of the wireless system before production implementation including the creation of a Wireless Security Plan (Reference http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf for guidance);
- Maintain a current, documented diagram of the topology of the wireless network;
- Label and keep an inventory of the wireless and handheld devices;
- Perform periodic security testing and assessment of the wireless network;
- Perform ongoing, randomly timed security audits to monitor and track wireless laptop and handheld PDA usage on the network to ensure only authorized users are utilizing the network;
- Implement configuration/change control and management to ensure that equipment has the latest software release that includes security enhancements and patches for discovered vulnerabilities;
- Implement standardized configuration to reflect the Wireless Security Plan, to ensure change of default values, and to ensure consistency of operation;
- Implement security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies;
- Monitor the wireless industry for changes to standards that enhance security features and for the release on new products;
- Vigilantly monitor wireless technology for new threats and vulnerabilities;
- Wireless networks must implement some form of cryptographic protocol, examples being secure shell (SSH), Transport-Level Security (TLS), Internet Protocol Security (IPsec), or Virtual Private Networks (VPN);
- Additional countermeasures such as strategically locating access points, ensuring firewall filtering, blocking, and the installation of antivirus software must be implemented.

7.8.2 Wireless Security Plan

The Wireless Security Plan must do the following:

- Identify who may use the technology in the agency;
- Identify whether Internet access is required;
- Describe who can install access points and other wireless equipment;
- Provide limitation on the location of and physical security for access points;
- Describe the type of information that may be sent over wireless links;
- Describe the conditions under which wireless devices are allowed;
- Define standard security settings for access points;
- Describe limitation on how the wireless devices may be used;
- Describe the hardware and software configuration of all wireless devices;
- Provide guidelines on reporting losses of wireless devices and security incidents;
- Provide guidelines for the protection of wireless clients to minimize/reduce theft;
- Define the frequency and scope of security assessments to include access point discovery.

Access Point Configuration

- All default passwords must be changed to comply with the State of Maryland password policies before production implementation;
- The Secure Set Identifier (SSID) must be changed from the factory default before production implementation;
- The beacon interval which announces the existence of a wireless network should be set to its highest value;
- Disable the broadcast SSID feature;
- Change default cryptographic keys;
- If SNMP is not required, the agency should disable it;
- If SNMP is required, agencies must use SMNPv3 or higher;
- Dynamic Host Control Protocol (DHCP) should be disabled and static IP addresses should be used on the wireless network, if feasible, and/or utilize access points with integrated firewalls.

Authentication

- The access point must verify the identity of the wireless device (i.e., open-system authentication and WEP and WEP2 are prohibited).

Intrusion Detection/Prevention Systems

- Host Based Intrusion Detection System (IDS) or Intrusion Prevention Systems (IPS) must be implemented on the wireless network wherever possible.

7.9 Private Branch Exchange (PBX)

If PBX processors require remote vendor maintenance via a dial-in telephone line the following controls must be in place:

- A single dedicated telephone line that disables access to the public-switched telephone network;
- An automated audit trail;
- Encryption of transmissions;
- Access controls.

7.10 Facsimile

Data transmitted by facsimile must be treated in the same manner as any data communicated by network or PBX based on system sensitivity and data classification.

Section: 8	Revision: 2
Date Adopted: June 2003	Date Revised: December 2005

8 Physical Security Standard

Physical access to IT information processing, storage areas, and storage devices and its supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas. Agencies must:

- Secure IT areas with controls commensurate to the risks;
- Ensure the secure destruction of storage media;
- Ensure secure media reuse;
- Ensure secure storage of media;
- Obtain personnel security clearances where appropriate.

8.1 Secured IT Areas

Physical access controls must be in place for the following:

- Data Centers;
- Areas containing servers and associated media;
- Networking cabinets and wiring closets;
- Power and emergency backup equipment;
- Operations and control areas.

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be:

- Based on frequency of need for access;
- Approved by the manager responsible for the secured area.

Each agency is responsible for:

- Issuing picture id badges to all Employees/contractors and ensuring that these badges are openly displayed at all times;
- Ensuring that all portable storage media such as hard drives, flash media drives, diskettes, magnetic tapes, laptops, PDA devices, DVDs and CDs are physically secured;
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems;
- Ensuring that any physical access controls are auditable.

8.2 Storage Media Disposal

When no longer usable, diskettes, compact disks, tape cartridges, ribbons, and other similar items shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing (Ref: http://www.nsa.gov/ia/government/mdg.cfm?MenuID=10.3.1). No IT equipment shall be released from an agency's control until the equipment is sanitized and all stored information has been cleared. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient. This includes equipment transferred to schools, as well as equipment maintenance and repair.

8.3 Media Reuse

When no longer required for mission or project completion, media (tapes, disks, hard drives, etc.) to be

used by another person within the agency shall be overwritten with software and protected consistent with the data sensitivity of which the IT storage media were previously used. The procedures shall be documented in the IT System Security Plan.

8.4 Storage and Marking

IT Systems and electronic media shall be protected and marked in accordance with the data sensitivity. Users shall not store data on electronic media that cannot be adequately secured against unauthorized access. Data to be electronically transferred to a remote storage location should be transferred only by a secure and encrypted method.

8.5 Personnel

Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

Section: 9	Revision: 1
Date Adopted: June 2003	Date Revised: December 2005

9 Microcomputer/PC/Laptop Security Standard

Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes/stores data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices. To help accomplish this each agency must establish at a minimum the following:

- General controls;
- Virus protection;
- Software licensing and use controls;
- Laptop security and mobile computing controls;
- Protection from personally owned microcomputers and portable storage devices.

9.1 General Controls

All microcomputers that store and/or access nonpublic information must implement the following controls:
User id and password to control access at logon;

- Encryption to protect directories, sub-directories, and/or files containing nonpublic information;
- Virus Protection.

Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:

- Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing;
- Be updated as soon as updates are available from the vendor;
- Be configured to prevent connection to the network unless the accessing microcomputer has the latest version of the virus product and update installed.

9.2 Software Licenses and Use

Unless specifically approved by the Agency CIO and the agency head, personal or corporate IT equipment shall not have State licensed software installed and shall not be used to process or transmit nonpublic data. Only State owned and authorized computer software is to be used on standalone or networked computer equipment. The State will provide legally acquired software to meet legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.

Authorized software packages are those approved by the Agency CIO. Executable modules cannot be downloaded from the Internet unless authorized by the Agency CIO and agency network administrator. Agencies should designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

9.3 Laptop Security and Mobile Computing

Laptops and mobile computing devices are not authorized to process or store nonpublic information

unless approved in writing by the agency network support administrator, the Agency CIO and the agency head. Laptops and mobile computing devices which include personal digital assistants approved for processing nonpublic information cannot be connected to State networks or systems unless the network or system is certified and accredited for that function. In such cases the IT Security Program will identify the devices that can be used to access the network or the system, the purposes for the access, and the security controls for the connection.

9.4 Personally Owned Data Processing Equipment

Personal or contractor owned data processing and data storage equipment (i.e., not owned by the State) are prohibited from accessing systems with nonpublic information and processing or storing nonpublic information unless approved by the agency network support administrator and the Agency CIO.

Section: 10	Revision: 1
Date Adopted: June 2003	Date Revised: December 2005

10 Encryption Standard

Agencies must ensure that encryption is utilized to protect any nonpublic information when it is stored or transmitted through any environment. IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (Reference http://csrc.nist.gov/publications/fips/ for guidance).

To help accomplish this each agency using encryption must establish at a minimum the following:

- Secure cryptographic keys;
- Use of Public Key Cryptography methods approved by the State CIO;
- All cryptographic keys must have a designated, unique owner.

Key change intervals shall be established by each agency, but must be no longer than the following:

- Master keys must be changed once per year, if the product allows;
- Key encrypting keys (e.g., asymmetric encrypting a symmetric) must be changed at a minimum of every six (6) months;
- Link encrypting keys must be changed every six (6) months.

Keys must be distributed in a secure manner ensuring that the entire key is not exposed while in transit to any one individual at any one time.

Default cryptographic keys may not be utilized. Exceptions are for emergency recovery, system calibration or vendor certification purposes. In such cases, a documented process describing the storage, maintenance, use and destruction of these keys must be in place.

10.1 Public Key Technology (Asymmetric)

All public key management systems, Certificate Authorities (CAs), key distribution systems, key recovery systems, and cross-certification processes must be approved by the State CIO. Every public key and certificate must have an associated scope of use, which must be checked by any user or server that accepts or relies upon the certificate.

The process for issuing digital certificates must:

- Establish the identity of the subject;
- Establish that the subject is the holder of the associated private keys;

Section: 11	Revision: 2
Date Adopted: June 2003	Date Revised: December 2005

11 IT Information Security Deviation/Risk Acceptance Standard

An Information Security Deviation Request/Risk Acceptance form must be completed by the agency if it determines that it cannot or will not comply with the State IT Security Policy. All deviation requests require the approval of the agency CIO, agency head, and the State CIO.

11.1 General Requirements

- Proposed deviations will be considered on an individual basis;
- Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures and extenuating circumstances associated with the proposed deviation and its impact on IT systems;
- Requests for deviations must be made in writing;
- Deviations will be granted for a maximum period of twelve (12) months after which time the deviation will be considered expired and require renewal.

Section: 12	Revision: 1
Date Adopted: June 2003	Date Revised: December 2005

12 Use of Electronic Communications Standard

This standard applies to information technology security, however, it is not inclusive of other State policies and regulations that may further apply to the use of electronic communications.

The use of the Internet, E-mail and other State computing equipment, networks and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. Information communicated electronically through email, the Internet or sharing of electronic documents is subject to State laws, regulations, policies and other requirements, as is information communicated in other written forms and formats. Access to State agency email or Internet services may be wholly or partially restricted without prior notice and without user consent.

12.1 Internet and Electronic Communications

Users accessing the Internet or other State electronic communications through State resources may be monitored. Agencies shall develop standards consistent with all State policies and standards regarding E-mail, Internet use, and use of other computer resources. Electronic communications that are not secure or encrypted should not be used to send information that is nonpublic information.

12.2 Computer Software and Copyright Infringement

The State will not permit the making or using of unauthorized software copies under any circumstances. This includes, but is not limited to programs, executable modules and screen savers (e.g. downloaded software, pirated software, software not licensed to the State, software brought from home). Agencies will establish and enforce internal controls to prevent the making or use of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards. For additional guidance refer to Annotated Code of Maryland, Criminal Law, Section 7-302**.**

The Agency CIO is responsible for ensuring that the agency is abiding by the terms of all software licenses and for compliance with the prevention of software copyright infringement and protection. The Agency CIO, or designee, shall establish and maintain positive control of software, including inventory measures and accounting procedures that document all purchases of software. Each agency shall establish written procedures that include at a minimum the following:

- Control of all software and software licenses;
- A program that informs employees about the need to comply with software licenses;
- Requirement for all employees to sign the State of Maryland Software Code of Ethics (Attachment 1).

12.3 IT Incident and Advisories

Each agency shall notify its staff of the personnel designated to provide authenticated notices of IT incidents and advisories. Employees other than the designated personnel shall not forward IT Incident advisories to agency staff. If an advisory comes to an employee, the employee shall forward it to the designated personnel for evaluation.

13 Record of Revisions

Issue	Date	Section	Description
Revision 1.3	December 2005	Cover Page	Modified date and revision
		1	Changed Format
		1.1, 1.4	Removed reference to Executive Order
		1.6	Added language: guidance and reference
		2	Changes format, added terms and definitions: IPS, Untrustred Network, VoIP
		3	Changed format
		3.1	Added Enforcing State security policy
		4	Changed format
		4.9	Removed reference to State Data Security Committee
		6	Removed bullet line 6
		6.1.1	Changed bullet line 9 to reflect 90 days for general users. Changed line 11 to allow for a 10 minute automatic reset
		6.2	Changed bullet line 5: removed the 90 removal reference
		7	Changed format, added VoIP
		7.4	Added Intrusion Prevention System
		7.8	Added language: guidance. Added IPS reference
		8	Changed format
		8.2	Removed reference to second URL “Miami.edu”
		8.4	Added reference to secure and encrypted method.
		9	Changed format
		9	Added “processes/stores”
		9.2	Removed reference to DBM
		10	Changed format, changed language to state “reference”, “guidance”.

Issue	Date	Section	Description
		11	Changed format
		12	Changed format
		12.2	Changed heading, added paragraph to cover SCOE position.
		13 (old)	Removed
		14	Changed to Section 13
			Added Revision references for 2005
		14	Appended Software Code of Ethics attachment
Revision 1.2	December 2004	1.7	Agency deviation approval list modified
		2	Mobile Code definition added, Nonpublic Definition added,
			PPI Definition removed and all references to PPI changed to nonpublic.
		7.8	Wireless Network Controls, Security Plan, A.P. Configuration, Authentication, IDS.
		8.2	Storage Media Disposal
		9.4	Personally Owned Data Processing Equipment.
		11.1	Requests for deviations format
Revision 1.1	July 24, 2003	7.2	Banner Text modified.
Policy issued	June 6, 2003	N/A	N/A

ATTACHMENT 1
STATE OF MARYLAND
SOFTWARE CODE OF ETHICS

Unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct. The State disapproves of such copying and recognizes the following principles as a basis for preventing its occurrence.

1. The State will not permit the making or using of unauthorized software copies under any circumstances.

2. The State will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.

3. The State will enforce internal controls to prevent the making or using of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards.

My signature indicates that I have read and understand this State of Maryland Software Code of Ethics. I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making or using unauthorized software may also subject me to civil and criminal penalties.

SIGNATURE: _____ DATE: _____

NAME: (Please Print): _____

AGENCY: _____

DIVISION: _____

LOCATION: _____